R E P U B L I Q U E F R A N Ç A I S E

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

PCT/FR03/02074

REC'D 30 SEP 2003
WIPO PCT

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 08 JUIL. 2003

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS CONFORMÉMENT À LA RÈGLE 17.1.a) OU b)

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*01

REQUÊTE EN DÉLIVRANCE 1/2

Cet imprimé est à remplir lisiblement à l'encre noire DB 540 W / 190600

Réservé à l'INPI

REMISE DES PIÈCES
DATE 4 JUIL 2002
LIEU 75 INPI PARIS B
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0208418
DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 04 JUIL. 2002

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

ARMENGAUD JEUNE
CABINET LEPEUDRY
43, rue de la Brèche aux Loups
75012 PARIS

Vos références pour ce dossier *(facultatif)* Eracofa

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie

2 NATURE DE LA DEMANDE	Cochez l'une des 4 cases suivantes
Demande de brevet	☒
Demande de certificat d'utilité	☐
Demande divisionnaire	☐
Demande de brevet initiale	N° Date / /
ou demande de certificat d'utilité initiale	N° Date / /
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N° Date / /

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Procédé et système de sécurisation de transmission de messages.

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE	
	Pays ou organisation Date / / N°
	Pays ou organisation Date / / N°
	Pays ou organisation Date / / N°
	☐ S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»

5 DEMANDEUR	☐ S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»
Nom ou dénomination sociale	ERACOFA SAS
Prénoms	
Forme juridique	Société en formation
N° SIREN	
Code APE-NAF	
Adresse — Rue	
Adresse — Code postal et ville	
Pays	FRANCE
Nationalité	française
N° de téléphone *(facultatif)*	
N° de télécopie *(facultatif)*	
Adresse électronique *(facultatif)*	

Remplir impérativement la 2ème page

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

N° 11354*02

REQUÊTE EN DÉLIVRANCE
page 1/2

BR1

Cet imprimé est à remplir lisiblement à l'encre noire

DB 540 @ W / 010801

Réservé à l'INPI	
REMISE DES PIÈCES DATE 4 JUILLET 2002 LIEU 75 INPI PARIS N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0208418 DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI	1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE ARMENGAUD JEUNE CABINET LEPEUDRY 43, rue de la Brèche aux loups 75012 PARIS
Vos références pour ce dossier *(facultatif)* ERACOFA	

Confirmation d'un dépôt par télécopie	☐ N° attribué par l'INPI à la télécopie
2 NATURE DE LA DEMANDE	**Cochez l'une des 4 cases suivantes**
Demande de brevet	☒
Demande de certificat d'utilité	☐
Demande divisionnaire	☐
Demande de brevet initiale	N° Date
ou demande de certificat d'utilité initiale	N° Date
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N° Date

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Procédé et système de sécurisation de transmission de messages.

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE	Pays ou organisation Date N° Pays ou organisation Date N° Pays ou organisation Date N° ☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**
5 DEMANDEUR (Cochez l'une des 2 cases)	☐ **Personne morale** ☒ **Personne physique**
Nom ou dénomination sociale	SUANEZ
Prénoms	Roger
Forme juridique	Agissant au nom et pour le compte de la Société ERACOFA SA en cours de formation
N° SIREN	
Code APE-NAF	
Domicile ou siège — Rue	36, rue du Bois
Code postal et ville	44510 LE POULIGUEN
Pays	FRANCE
Nationalité	
N° de téléphone *(facultatif)*	N° de télécopie *(facultatif)*
Adresse électronique *(facultatif)*	

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE 2/2

Réservé à l'INPI

REMISE DES PIÈCES
DATE
LIEU 4 JUIL 2002
75 INPI PARIS B
N° D'ENREGISTREMENT
NATIONAL ATTRIBUÉ PAR L'INPI 0203418

DB 540 W / 190600

Vos références pour ce dossier : *(facultatif)*		
6 MANDATAIRE		
Nom		
Prénom		
Cabinet ou Société		ARMENGAUD JEUNE CABINET LEPEUDRY
N °de pouvoir permanent et/ou de lien contractuel		
Adresse	Rue	43, Rue de la Brèche aux Loups
	Code postal et ville	75012 PARIS
N° de téléphone *(facultatif)*		
N° de télécopie *(facultatif)*		
Adresse électronique *(facultatif)*		
7 INVENTEUR (S)		
Les inventeurs sont les demandeurs		☐ Oui ☒ Non **Dans ce cas fournir une désignation d'inventeur(s) séparée**
8 RAPPORT DE RECHERCHE		**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé		☒ ☐
Paiement échelonné de la redevance		**Paiement en deux versements, uniquement pour les personnes physiques** ☐ Oui ☐ Non
9 RÉDUCTION DU TAUX DES REDEVANCES		**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Requise antérieurement à ce dépôt *(joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence) :*
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		

10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE
(Nom et qualité du signataire)

LEPEUDRY Thérèse n° 92-1152

VISA DE LA PRÉFECTURE OU DE L'INPI
M. MARTIN

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE
page 2/2

BR2

Réservé à l'INPI

REMISE DES PIÈCES
DATE 4 JUILLET 2002
LIEU 75 INPI PARIS

N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0208418

DB 540 @ W / 010801

Vos références pour ce dossier : *(facultatif)*		ERACOFA
6 **MANDATAIRE** *(s'il y a lieu)*		
Nom		
Prénom		
Cabinet ou Société		CABINET LEPEUDRY
N °de pouvoir permanent et/ou de lien contractuel		
Adresse	Rue	43, rue de la Brèche aux Loups
	Code postal et ville	7 5 0 1 2 PARIS
	Pays	FRANCE
N° de téléphone *(facultatif)*		01 43 44 69 90
N° de télécopie *(facultatif)*		01 43 42 04 92
Adresse électronique *(facultatif)*		
7 **INVENTEUR (S)**		**Les inventeurs sont nécessairement des personnes physiques**
Les demandeurs et les inventeurs sont les mêmes personnes		☐ Oui ☒ Non : **Dans ce cas remplir le formulaire de Désignation d'inventeur(s)**
8 **RAPPORT DE RECHERCHE**		**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé		☒ ☐
Paiement échelonné de la redevance *(en deux versements)*		**Uniquement pour les personnes physiques effectuant elles-mêmes leur propre dépôt** ☐ Oui ☐ Non
9 **RÉDUCTION DU TAUX DES REDEVANCES**		**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Obtenue antérieurement à ce dépôt pour cette invention *(joindre une copie de la décision d'admission à l'assistance gratuite ou indiquer sa référence)* : **AG**
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		1

10 **SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire)**

LE PEUDRY Thérèse - n° 92-1152

VISA DE LA PRÉFECTURE OU DE L'INPI

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*0

REQUÊTE EN DÉLIVRANCE

Page suite N° 1 / 2

BR/SUI

Réservé à l'INPI

REMISE DES PIÈCES
DATE 4 JUILLET 2002
LIEU 75 INPI PARIS

N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0208418

Cet imprimé est à remplir lisiblement à l'encre noire

DB 829 @ W / 1806

Vos références pour ce dossier *(facultatif)*		ERACOFA
4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE		Pays ou organisation Date |_|_|_|_|_|_|_|_| N° Pays ou organisation Date |_|_|_|_|_|_|_|_| N° Pays ou organisation Date |_|_|_|_|_|_|_|_| N°
5 DEMANDEUR (Cochez l'une des 2 cases)		☐ **Personne morale** ☒ **Personne physique**
Nom ou dénomination sociale		ETIENNE
Prénoms		Patricia
Forme juridique		agissant au nom et pour le compte de la Société ERACOFA SA en cours de
N° SIREN		|_|_|_|_|_|_|_|_|_| de formation
Code APE-NAF		|_|_|_|_|
Domicile ou siège	Rue	36, rue du Bois
	Code postal et ville	|4|4|5|1|0| LE POULIGUEN
	Pays	FRANCE
Nationalité		Française
N° de téléphone *(facultatif)*		
N° de télécopie *(facultatif)*		
Adresse électronique *(facultatif)*		
5 DEMANDEUR (Cochez l'une des 2 cases)		☒ **Personne morale** ☐ **Personne physique**
Nom ou dénomination sociale		ERACOFA SA, représenté par son Président GAULIS Etienne agissant en cette qualité
Prénoms		
Forme juridique		Société de droit suisse - Agissant au nom et pour le compte de la Société
N° SIREN		|_|_|_|_|_|_|_|_|_| ERACOFA SA en cours de formation
Code APE-NAF		|_|_|_|_|
Domicile ou siège	Rue	Etablissement Fontannins 28
	Code postal et ville	|1|0|6|6| EPALINGE
	Pays	SUISSE
Nationalité		Suisse
N° de téléphone *(facultatif)*		
N° de télécopie *(facultatif)*		
Adresse électronique *(facultatif)*		

10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire)

LE PEUDRY Thérèse - n° 92-1152

VISA DE LA PRÉFECTURE OU DE L'INPI

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.

La présente invention concerne un procédé et système de sécurisation de transmission de messages.

Il est connu dans la sécurisation de message d'effectuer la signature d'un message et de transmettre celle-ci accolée au message pour permettre à un dispositif récepteur possédant la clé appairée à la clé ayant permis la génération de signatures du message soit de déchiffrer le message signé soit de calculer à partir de cette clé appairée une autre signature et de la comparer à la signature reçue. Par clé appairée, il faut comprendre soit la clé publique associée à une clé privée d'un algorithme de chiffrement à clé publique, soit deux clés secrètes connues l'une d'une première entité permettant le chiffrement d'un message envoyé, respectivement le déchiffrement d'un message reçu d'une autre entité disposant de la deuxième clé permettant le déchiffrement des messages reçus de la première entité ou le chiffrement des messages émis vers la première entité.

Ces techniques de chiffrement des communications sous protocole sécurisé par cryptographie asymétrique (par exemple publique) ou symétrique ont l'inconvénient qu'à la fin du cycle de transport les contenus dématérialisés et signés ne sont pas toujours au rendez-vous et l'organisme récepteur n'est pas en mesure de certifier que le message reçu correspond parfaitement à celui émis et qu'entre autre l'autorité qui s'auto-certifie ne peut pas valablement prouver l'intégrité des contenus lorsqu'ils ont fait l'objet d'altération accidentelle ou préméditée durant un cycle de leur transfert. En effet, il peut arriver que le message et la signature puissent être soit fortuitement soit volontairement altérés dans le même sens et que l'altération ainsi générée ne puisse pas être détectée en fin de cycle d'auto-certification. Le but de l'invention est donc de

proposer un système permettant de vérifier avec certitude que la signature correspondant à un message envoyé n'a pas été fortuitement ou volontairement altérée en adjoignant à cette signature une information supplémentaire sur laquelle la vérification peut s'établir.

Ce but est atteint par le fait que le procédé de sécurisation de la transmission de messages comporte une étape de transmission du message et de sa signature et d'adjonction au message signé d'une information cryptée ou non d'identification de l'émetteur et d'une information supplémentaire découlant du message ;

une étape de transmission de l'ensemble ;

une étape de réception par le récepteur et de détermination de l'information cryptée ou non d'identification de l'émetteur puis d'utilisation de cette information d'identification de l'émetteur pour déterminer une information découlant également du message déchiffré et de comparaison de l'information découlant du message déchiffré avec l'information découlant du message mais transmise de l'émetteur vers le récepteur préalablement calculé à la transmission par l'émetteur.

Selon une autre particularité, l'information découlant du message est représentative de la consistance du message et de la signification du message.

Selon une autre particularité, la consistance du message est déterminée en divisant l'information d'identification de l'émetteur par le nombre de caractères contenu dans le message.

Selon une autre particularité, le reste obtenu par la division précédente est lui-même divisé par un nombre premier pour obtenir un quotient et un deuxième reste, le deuxième reste étant ajouté à une constante pour obtenir un nombre de caractères identique quelle que soit la base de

conversion choisie comprise parmi une pluralité de bases de conversion.

Selon une autre particularité, la signification du message est déterminée par la somme d'un nombre n d'éléments, chaque élément étant constitué du double de la valeur ASCII représentative du caractère précédent du message, diminuée de la valeur ASCII représentative du caractère suivant du message, cette somme servant de diviseur d'un dividende constitué par l'information d'identification.

Selon une autre particularité, le reste du quotient précédent est divisé par un nombre premier pour obtenir un quotient et un troisième reste dont la valeur est ajoutée d'une valeur constante.

Selon une autre particularité, le nombre premier est 46027, la constante est 4623.

Selon une autre particularité, la consistance du message est représentée par un nombre de digits faible (par exemple 3) dans l'information transmise.

Selon une autre particularité, la signification du message est représentée par un nombre de digits faible dans l'information transmise.

Selon une autre particularité, l'information d'identification est obtenue à partir de chaînes de caractères et de valeurs numériques de taille déterminée représentant des rubriques à protéger en réalisant une étape de condensation de ces chaînes en plusieurs nombres de p chiffres de taille inférieure au nombre représentatif de la taille des chaînes pour constituer un premier ensemble de m résultats intermédiaires de p chiffres ;

une étape de transformation de ces m résultats intermédiaires par un algorithme tiré aléatoirement parmi plusieurs, en un deuxième résultat de p chiffres exprimé en base 10 élaboré par une matrice de conversion des caractères

d'une base alphanumérique en caractères numériques d'une base décimale mémorisée sur le système de calcul.

Selon une autre particularité, cette information d'identification est transmise sous forme cryptée en transformant cette information d'identification en base 10 en un résultat crypté, un même p de chiffres exprimés dans une même base mathématique choisie aléatoirement par le système parmi un choix déterminé de bases de conversion disponibles et mémorisées par le système de calcul pour obtenir un identifiant crypté auquel on ajoute des informations de détermination de la base mathématique en insérant dans ce résultat crypté le caractère qui, exprimé dans la base, détermine la base utilisée pour déterminer le résultat crypté par insertion chronologique de ce caractère parmi les caractères qui représentent ce résultat à un rang défini par le quotient entier de la division du caractère déterminant la base utilisée par le nombre s définissant le nombre d'algorithmes, le reste de cette division activant l'algorithme choisi pour calculer l'information d'identification.

Selon une autre particularité, le caractère est inséré à un rang, soit prédéfini, soit calculé en prenant le modulo 9 de la somme des codes ASCII d'une troncature d'une ou plusieurs chaînes de caractères et de valeurs numériques de taille déterminée représentant les termes de la fonction mathématique déterminant l'information d'identification et transmise avec le message sous forme cryptée ou non.

Selon une autre particularité, le système récepteur comporte une étape de calcul de la somme des codes ASCII d'une ou plusieurs troncatures de rubrique alphabétique reçue dans l'information d'identification puis de calcul du modulo 9 de cette somme pour déterminer la position du caractère aléatoire puis de lecture de ce caractère reçu et de calcul du rang de la position de la valeur de la base en

divisant cette valeur par la valeur du nombre d'algorithmes de calcul du résultat intermédiaire de l'information d'identification, exprimée en base décimale en éliminant des informations cryptées reçues la position représentative du caractère de base et la position représentative du caractère aléatoire.

Selon une autre particularité, le procédé comprend une étape de calcul de l'information de consistance de l'information de signification du message par utilisation de l'information d'identification déterminée à l'étape précédente et exprimé en base 10.

Selon une autre particularité, le procédé comprend une étape de comparaison des résultats calculés par le dispositif récepteur avec les résultats reçus transmis en même temps que le message et après avoir extrait des résultats transmis une certaine troncature.

Un autre but de l'invention est de proposer un système de sécurisation de transmission.

Ce but est atteint par le fait que le système de sécurisation de transmission comporte un dispositif émetteur comportant des moyens de déterminer une information d'identification de l'émetteur et de déterminer d'une information découlant du message, d'adjoindre ces informations d'identification découlant du message au message signé, de transmettre ce message signé, et du côté du récepteur des moyens de calculer à partir de l'information d'identification une information intermédiaire permettant de recalculer à partir de la signature déchiffrée du message une nouvelle information de consistance et une nouvelle information de signification à comparer aux informations de consistance de signification reçues avec le message, et des moyens de comparaison et de mémorisation des informations calculées et reçues. Le système émetteur

comporte un algorithme permettant d'effectuer les calculs précédents.

Selon une autre particularité, le système récepteur comporte l'algorithme permettant d'effectuer les calculs correspondant à sa fonction et de mémoriser les étapes intermédiaires.

L'invention, avec ses caractéristiques et avantages, ressortira plus clairement à la lecture de la description faite en référence aux dessins annexés dans lesquels :

- la figure 1 représente les moyens nécessaires à la mise en œuvre de l'invention constitués d'un émetteur, d'un récepteur et d'une ligne de transmission de messages entre l'émetteur et le récepteur,
- la figure 2 représente schématiquement une vue de détail des opérations qui se déroulent au niveau du récepteur,
- la figure 3 représente schématiquement une vue de détail des informations d'élaboration du chiffrement de protection des documents qui se déroulent au niveau de l'émetteur,
- la figure 4 représente les étapes de détermination d'une information d'identification (IDENT_SPY) pour utilisation dans les opérations de la figure 2 à partir de l'information d'identification cryptée.

L'invention va à présent être décrite en liaison avec les figures 1 à 4.

Il était connu dans l'art antérieur de la transmission d'informations entre un terminal émetteur et un terminal récepteur informatique sur une ligne de communication, de faire effectuer un calcul par l'émetteur sur le message (M) en utilisant une clé secrète pour réaliser un calcul de signature (S) sur le message (M), d'adjoindre cette signature au message, éventuellement de chiffrer (C) l'ensemble et de transmettre l'ensemble ($(M,S)^c$) de ces

informations sur la ligne de transmission vers le récepteur. De son côté, le récepteur par utilisation d'un algorithme de déchiffrement symétrique ou asymétrique va déchiffrer si nécessaire l'ensemble des informations reçues pour retirer de ce déchiffrement une information qu'il sépare en deux informations, une première qu'il considèrera comme la signature reçue, une deuxième comme représentant le message. Le terminal récepteur effectue sur cette deuxième information le même calcul que celui effectué par l'émetteur, pour déterminer une nouvelle signature (S') dont le résultat sera comparé à la signature (S) reçue. Le récepteur considérait une fois cette comparaison réussie que le message reçu correspondait à celui émis. Toutefois ce système n'était pas infaillible car, par exemple, il suffisait au fraudeur soit d'inverser deux caractères dans le message, ce qui ne se détectait pas dans la signature, soit de substituer totalement un nouveau message et une nouvelle signature à l'ensemble et le récepteur considérait les informations reçues comme étant authentiques.

Le procédé mis en œuvre par l'invention consiste à faire calculer par le terminal émetteur une information d'identification (IDENT_SPY) que celui-ci peut éventuellement crypter (CRYPT_IDENT° dans une base de calcul déterminée de façon aléatoire et à laquelle l'émetteur ajoute des informations permettant de retrouver la base et des informations découlant du message (IDEM). L'ensemble de ces informations est ensuite transmis vers le terminal récepteur. Le récepteur à réception de ces informations va tout d'abord, si nécessaire, déchiffrer (C-1) la partie chiffrée du message puis calculer une signature (S') en utilisant le message (M) déchiffré et la comparer avec la signature reçue (S). Dans le cas où cette comparaison est positive, le récepteur poursuit son processus de validation du message en déterminant à partir des informations

d'identification cryptée, celles qui permettent de retrouver la base (Y) de calcul de la valeur d'une information d'identification appelée IDENT_SPY, constituée d'une suite de chiffres, par exemple de l'ordre de 11-12 chiffres. Cette information d'identification (IDENT_SPY) est combinée par le terminal au nombre de caractères du message pour en déduire une information (X'') sur la consistance du message. La même information (IDENT_SPY) est combinée aux valeurs ASCII représentatives de chacun des caractères du message pour en déduire une information sur la signification (Y'') du message et comparer les informations (X'', Y'') calculées, de consistance et de signification du message aux informations (X', Y') reçues de consistance et de signification du message comprises dans l'information découlant du message (IDEM).

L'information (X') de consistance du message est calculée par le récepteur en appliquant l'algorithme suivant :

le récepteur utilise le nombre représentant l'information d'identifiant IDENT_SPY et divise ce nombre par la valeur représentative du nombre de caractères du message. Le reste ainsi obtenu est lui-même divisé par un nombre premier constitué, par exemple, par le nombre premier 46027. Le reste de cette division est ajouté à la valeur 4623 pour s'assurer que le résultat soit toujours compris dans des bornes de valeur permettant de coder ce résultat dans l'une des bases de la pluralité de bases sous un nombre de digits restreint, par exemple 3 digits.

La pluralité de bases de conversion peut être constituée par des bases comprises entre 37 et 127. La base 82, valeur moyenne des bases contenues dans l'étendue des caractères du code à barres 128, sert de référence d'évaluation de la robustesse moyenne de ce procédé contre la casse par force brutale. L'annexe 2 représente la base de

conversion 67 permettant la conversion des 67 caractères alphanumériques de la colonne (b67) en chiffres de la base 10 représentés à la colonne (b10) et vice-versa. L'annexe 1 représente la conversion des caractères en base 37 dans la base 10 et vice-versa.

Le système récepteur utilise également l'information d'identification (IDENT_SPY) comme dividende pour faire diviser cette valeur par la somme d'un nombre d'éléments correspondant au nombre de caractères du message. Chaque élément est le double de la valeur ASCII d'un caractère (n) diminuée de la valeur ASCII du caractère suivant (n+1). Le reste ainsi obtenu est lui-même divisé par la valeur 46027 représentation d'un nombre premier et le reste obtenu est ajouté à la valeur 4623 pour déterminer une valeur représentée dans l'une des bases choisies, par exemple en base 37 ou en base 67 sous forme de 3 digits. Ces valeurs X'' et Y'' calculées sont comparées aux valeurs X' et Y' transmises avec le message M et ayant été calculées préalablement à la transmission du message par l'émetteur. La valeur Y', comme on le comprendra par l'exemple ci-après, est déterminée de telle façon que la valeur du nombre IDENT_SPY, fixée pour le contrôle de la capacité des registres de la mémoire, est étendue dans cet exemple entre 32259945714 et 32259948772 lorsqu'il est divisé par le dividende qui est constitué à partir de la valeur ASCII des caractères comme on l'a expliqué précédemment peut donc prendre comme valeur, dans cet exemple, entre 003210985 et 333210952. Puis lorsque l'on divise le reste obtenu par cette division par le nombre premier 46027, on obtient un second reste auquel il est ajouté la valeur constante 4623. On obtient dans le premier cas la valeur 4623 en base 10 qui transformée en base 37 vaut « 3dz » et en base 67, « 120 ». Dans le deuxième cas on obtient 50649 en base 10, ce qui représenté en base 37 prend la valeur AAx, et en base 67 la

valeur bif. Les trois informations (l'information d'identification (CRYPT_IDENT) et les informations de consistance (X') et la signification (Y') du message) ainsi rajoutées au message, constituent pour la première une information qui se distingue indépendamment des deux suivantes. Cette information d'identification est obtenue d'une troncature de plusieurs caractères de poids plus fort parmi lesquels se trouve placé à un rang tiré aléatoirement le caractère représentant la base mathématique d'expression du résultat du calcul.

Ce premier résultat constitue un condensé identitaire d'une personne physique ou morale ou d'un document ou d'un objet obtenu par application d'un algorithme de calcul (As) tiré aléatoirement parmi plusieurs (s) et dont les différents termes et constantes de la fonction mathématique sont constitués de nombres convertis, exprimés en base décimale et provenant des différentes rubriques alphabétiques et numériques identifiant la personne morale, la personne physique, l'objet, le document ou l'information à authentifier dans la transmission.

La seconde information X' découle du contenu du document dématérialisé et fournit la preuve de sa consistance en vérifiant que le message contient bien les n caractères prévus et cette seconde information est exprimée par la fonction (F1) :

$$\text{IDENT\_SPY MOD} \sum_{Ci=1}^{Ci=n} C_i \bmod 46027 + 4623 = X'$$

La troisième information Y' découle aussi du contenu du message et fournit la preuve de son sens ou de sa signification en reposant sur la valeur ASCII de chacun des caractères composant le message. Cette troisième information est obtenue par la formule (F2) :

$$\text{IDENT\_SPY MOD} \sum_{Ci=1}^{Ci=n-1} (2 \text{ val ASCII } C_i - \text{ val ASCII } C_{i+1}) \bmod 46027 + 4623 = Y'$$

Ces deux derniers résultats concaténés (X', Y') forment une seconde troncature de poids plus faible qui concaténée à la première troncature (CRYPT_IDENT) est concaténée au message signé (M, S). La première troncature (CRYPT_IDENT) confirme l'identité du signataire du message dématérialisé et déchiffré, la seconde (X', Y') permet sa validation ou sa répudiation en cas d'altération pour causes multiples du contenu chiffré.

Le système et procédé décrit peut s'appliquer également pour des paiements électroniques effectués par titre au porteur pourvu d'une zone grattable ou autre découvrant la seconde troncature (X', Y') qui doit alors contenir un code aléatoire résultant du calcul effectué pour valider les références de chacun des titres.

Le principe d'élaboration du premier résultat déjà exposé dans une demande précédente déposée par le même inventeur, constituée par la demande PCT/FR 01/04200 maintenant être explicitée en liaison avec les figures 3 et 4 pour permettre une meilleure compréhension de la présente invention.

Un premier résultat est élaboré à partir de chaînes de caractères Ch1 à Ch4 et de chaînes de valeurs numériques Ch5 à Ch7, représentant des rubriques à protéger pour identifier des falsifications sur des informations ou des documents ou des identités de personnes physiques ou morales, ou d'objets. Ces chaînes (Ch1 à Ch7) sont ensuite condensées en une pluralité (11 à 14) de résultats intermédiaires comportant chacun un nombre p de chiffres déterminés inférieurs ou égaux au chiffre 9 de caractères et de valeurs numériques des chaînes (ch1 à ch7). Ces résultats intermédiaires sont transformés par un algorithme As tiré aléatoirement parmi plusieurs (s) en un deuxième résultat

(20) de p chiffres exprimé en base 10 élaboré par une matrice de conversion dans une base décimale mémorisée dans le système de calcul de l'émetteur. Ce résultat (20) en base décimale constitue l'information d'identification (IDENT_SPY) utilisée ultérieurement pour déterminer la deuxième information (X') et la troisième information (Y'). Cette valeur exprimée en base 10 est ensuite transformée en une autre information (30) dite cryptée ayant un nombre constant de digits exprimés dans une base mathématique (Y) choisie aléatoirement par le système de calcul pour obtenir un identifiant crypté. La base (Y) est choisie aléatoirement par un algorithme de tirage aléatoire du système de calcul et parmi un certain nombre (V) de bases de conversion disponibles mémorisées par le système de calcul. Ces bases de calcul peuvent être comprises comme dans l'exemple donné entre les bases 37 et 67 qui figurent en annexes. Le nombre de bases peut s'étendre entre 37 et 127 ce qui correspond à un maximum de 91 bases, dont la valeur moyenne est 82. A cette valeur cryptée (30) est ajouté à un rang déterminé un caractère dont la valeur représente la base (Y) de conversion et le rang de ce caractère est fourni par une clé aléatoire (Z) elle-même disposée à un emplacement (W) déterminé soit par calcul, soit prédéterminé. Lorsque l'emplacement (W) est déterminé par calcul, celui-ci est effectué en prenant la somme en ASCII d'une ou plusieurs troncatures des rubriques alphanumériques d'une troncature de la chaîne de caractères Ch1 à Ch7 et en déterminant le modulo 9 de cette somme. Le reste ainsi obtenu par la division par 9 détermine la position du caractère qui permet de lire ensuite la clé aléatoire (Z), puis par division de cette clé aléatoire (Z) par une valeur (s) représentative du nombre d'algorithmes (As) de déterminer le rang (r) du caractère (Y) représentatif de la base de conversion. La base de conversion (Y) étant déterminée, le système

récepteur peut recalculer en sens inverse la valeur numérique en base 10 à partir du cryptogramme final CRYPT_IDENT après avoir occulté les positions r et W.

Les calculs ou tirages aléatoires effectués par l'un ou l'autre des terminaux émetteurs ou récepteurs peuvent être pris en charge en tout ou partie par une carte à puce communiquant avec le terminal. Ce terminal et la carte seront pourvus des algorithmes et des informations mémorisées nécessaires à amorcer la mise en œuvre de l'une des étapes du processus. Par exemple, la carte à puce peut contenir les tables de conversion et fournir les valeurs nécessaires au terminal. La carte peut aussi contenir les moyens de tirage aléatoire d'un algorithme parmi s et/ou de la table de conversion. La carte peut également contenir les algorithmes de décryptage pour obtenir l'information d'identification (IDENT_SPY) ou les algorithmes de cryptage pour déterminer la consistance (IDENT_SPY) à partir de Ch1 à Ch7. La carte peut également contenir les algorithmes de calcul de (X' ou X'') et de la signification (Y' ou Y''). Enfin, la carte peut contenir toute combinaison des possibilités ci-dessus.

On comprend ainsi l'intérêt de l'invention qui n'est nullement limitée aux bases de données indiquées, ni au nombre premier utilisé et encore moins aux nombres de caractères ou de troncatures présentés.

Il doit être évident pour les personnes versées dans l'art que la présente invention permet des modes de réalisation sous de nombreuses autres formes spécifiques sans l'éloigner du domaine d'application de l'invention comme revendiqué. Par conséquent, les présents modes de réalisation doivent être considérés à titre d'illustration mais peuvent être modifiés dans le domaine défini par la portée des revendications jointes.

ANNEXE 1

Matrice de la base 37

b37	b10
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
a	10
b	11
c	12
d	13
e	14
f	15
g	16
h	17
i	18
j	19
k	20
l	21
m	22
n	23
o	24
p	25
q	26
r	27
s	28
t	29
u	30
v	31
w	32
x	33
y	34
z	35
A	36

ANNEXE 2

Matrice de la base 67

b10	b67	b10	b67
0	0	34	y
1	1	35	z
2	2	36	A
3	3	37	B
4	4	38	C
5	5	39	D
6	6	40	E
7	7	41	F
8	8	42	G
9	9	43	H
10	a	44	I
11	b	45	J
12	c	46	K
13	d	47	L
14	e	48	M
15	f	49	N
16	g	50	O
17	h	51	P
18	i	52	Q
19	j	53	R
20	k	54	S
21	l	55	T
22	m	56	U
23	n	57	V
24	o	58	W
25	p	59	X
26	q	60	Y
27	r	61	Z
28	s	62	@
29	t	63	$
30	u	64	£
31	v	65	&
32	w	66	%
33	x		

REVENDICATIONS

1. Procédé de sécurisation de la transmission de messages caractérisé en ce qu'il comporte une étape de transmission du message et de sa signature et d'adjonction au message signé d'une information cryptée ou non d'identification de l'émetteur (CRYPTIDENT ou IDENT_SPY) et d'une information supplémentaire découlant du message (IDEM) ;

une étape de transmission de l'ensemble ;

une étape de réception par le récepteur et de détermination de l'information cryptée ou non d'identification de l'émetteur (CRYPTIDENT ou IDENT_SPY) puis d'utilisation de cette information d'identification de l'émetteur pour déterminer une information découlant du message déchiffré et de comparaison de l'information découlant du message déchiffré avec l'information découlant du message (IDEM) mais transmise de l'émetteur vers le récepteur préalablement calculé à la transmission par l'émetteur.

2. Procédé selon la revendication 1, caractérisé en ce que l'information découlant également du message (IDEM) est représentative de la consistance du message et de la signification du message.

3. Procédé selon la revendication 2, caractérisé en ce que la consistance du message est déterminée en divisant l'information d'identification (IDENT_SPY) de l'émetteur par le nombre n de caractères contenus dans le message.

4. Procédé selon la revendication 3, caractérisé en ce que le reste obtenu par la division précédente est lui-même divisé par un nombre premier pour obtenir un quotient et un deuxième reste, le deuxième reste étant ajouté à une constante pour obtenir un nombre de caractères identique

quelle que soit la base de conversion choisie parmi une pluralité de bases de conversion.

5. Procédé selon une des revendications 2 à 4, caractérisé en ce que la signification du message est déterminée par la somme d'un nombre n d'éléments, chaque élément étant constitué du double de la valeur ASCII représentative du caractère précédent du message, diminuée de la valeur ASCII représentative du caractère suivant du message, cette somme servant de diviseur d'un dividende constitué par l'information d'identification (IDENT_SPY).

6. Procédé selon la revendication 5, caractérisé en ce que le reste du quotient précédent est divisé par un nombre premier pour obtenir un quotient et un troisième reste dont la valeur est ajoutée à une valeur constante.

7. Procédé selon une des revendications 3 à 6, caractérisé en ce que le nombre premier est 46027, la constante est 4623.

8. Procédé selon un des revendications 2 à 7, caractérisé en ce que la consistance (X') du message est représentée par un nombre de digits faible dans l'information transmise.

9. Procédé selon une des revendications 2 à 7, caractérisé en ce que la signification (Y') du message est représentée par un nombre de digits faible dans l'information transmise.

10. Procédé selon une des revendications 1 à 9, caractérisé en ce que l'information d'identification (IDENT_SPY) est obtenue à partir de chaînes de caractères et de valeurs numériques de taille déterminée représentant des rubriques à protéger en réalisant une étape de condensation de ces chaînes en plusieurs nombres de p chiffres de taille inférieure au nombre (q) représentatif de la taille des chaînes pour constituer un premier ensemble de m résultats intermédiaires de p chiffres ;

une étape de transformation de ces m résultats intermédiaires par un algorithme (As) tiré aléatoirement parmi plusieurs (s) en un résultat final (IDENT_SPY) de p chiffres exprimé en base 10 élaboré par une matrice de conversion des caractères d'une base alphanumérique en caractères numériques d'une base décimale mémorisée sur le système de calcul.

11. Procédé selon la revendication 10, caractérisé en ce que l'information d'identification (IDENT_SPY) est transmise sous forme cryptée en transformant cette information d'identification en base 10 en un résultat crypté, un même nombre p de chiffres exprimés dans une même base mathématique (Y) choisie aléatoirement par le système parmi un choix (V) déterminé de bases de conversion disponibles et mémorisées par le système de calcul pour obtenir un identifiant crypté (CRYPT IDENT) auquel on ajoute des informations de détermination de la base mathématique (Y) en insérant dans ce résultat crypté le caractère qui, exprimé dans la base, détermine la base utilisée pour déterminer le résultat crypté par insertion chronologique de ce caractère parmi les caractères qui représentent ce résultat à un rang (r) défini par le quotient entier de la division du caractère (Z) déterminant la base (Y) utilisée par le nombre (s) définissant le nombre d'algorithmes, le reste de cette division activant l'algorithme choisi pour calculer l'information d'identification (IDENT_SPY).

12. Procédé selon la revendication 11, caractérisé en ce que le caractère (Z) est inséré à un rang, soit prédéfini, soit calculé en prenant le modulo 9 de la somme des codes ASCII d'une troncature d'une ou plusieurs chaînes de caractères et de valeurs numériques de taille déterminée représentant les termes de la fonction mathématique déterminant l'information d'identification (IDENT_SPY) et transmise avec le message (M) sous forme cryptée ou non.

13. Procédé selon une revendications 10 à 12, caractérisé en ce que le système récepteur comporte une étape de calcul de la somme des codes ASCII d'une ou plusieurs troncatures de rubrique alphabétique reçue dans l'information d'identification puis de calcul du modulo 9 de cette somme pour déterminer la position du caractère (Z) aléatoire puis de lecture de ce caractère (Z) reçu et calcul du rang (r) de la position de la valeur de la base (Y) en divisant cette valeur (Z) par la valeur (s) du nombre de d'algorithmes de calcul du résultat intermédiaire de l'information d'identification (IDENT_SPY), exprimée en base décimale en éliminant des informations cryptées reçues (CRYPT_IDENT) la position représentative du caractère de base (Y) et la position représentative du caractère aléatoire (Z).

14. Procédé selon la revendication 13, caractérisé en ce que le procédé comprend une étape de calcul de l'information de consistance de l'information de signification du message par utilisation de l'information d'identification (IDENT_SPY) déterminée à l'étape précédente et exprimé en base 10.

15. Procédé selon la revendication 14, caractérisé en ce que le procédé comprend une étape de comparaison des résultats calculés (X'', Y'') par le dispositif récepteur avec les résultats reçus (X', Y') transmis en même temps que le message et après avoir extrait des résultats transmis une certaine troncature (X', Y').

16. Système de sécurisation de transmission, caractérisé en ce qu'il comporte un dispositif émetteur comportant des moyens de déterminer une information d'identification de l'émetteur (IDENT_SPY) et de déterminer d'une information découlant du message, d'adjoindre ces informations d'identification découlant du message au message signé, de transmettre ce message signé, et du côté

du récepteur des moyens de calculer à partir de l'information d'identification une information intermédiaire (IDENT_SPY) permettant de recalculer à partir de la signature déchiffrée du message une nouvelle information de consistance et une nouvelle information de signification à comparer aux informations de consistance de signification reçues avec le message, et des moyens de comparaison et de mémorisation des informations calculées et reçues. Le système émetteur comporte un algorithme permettant d'effectuer les calculs précédents.

17. Système selon la revendication 16, caractérisé en ce que le système récepteur comportant l'algorithme permet d'effectuer les calculs correspondant à sa fonction et de mémoriser les étapes intermédiaires.

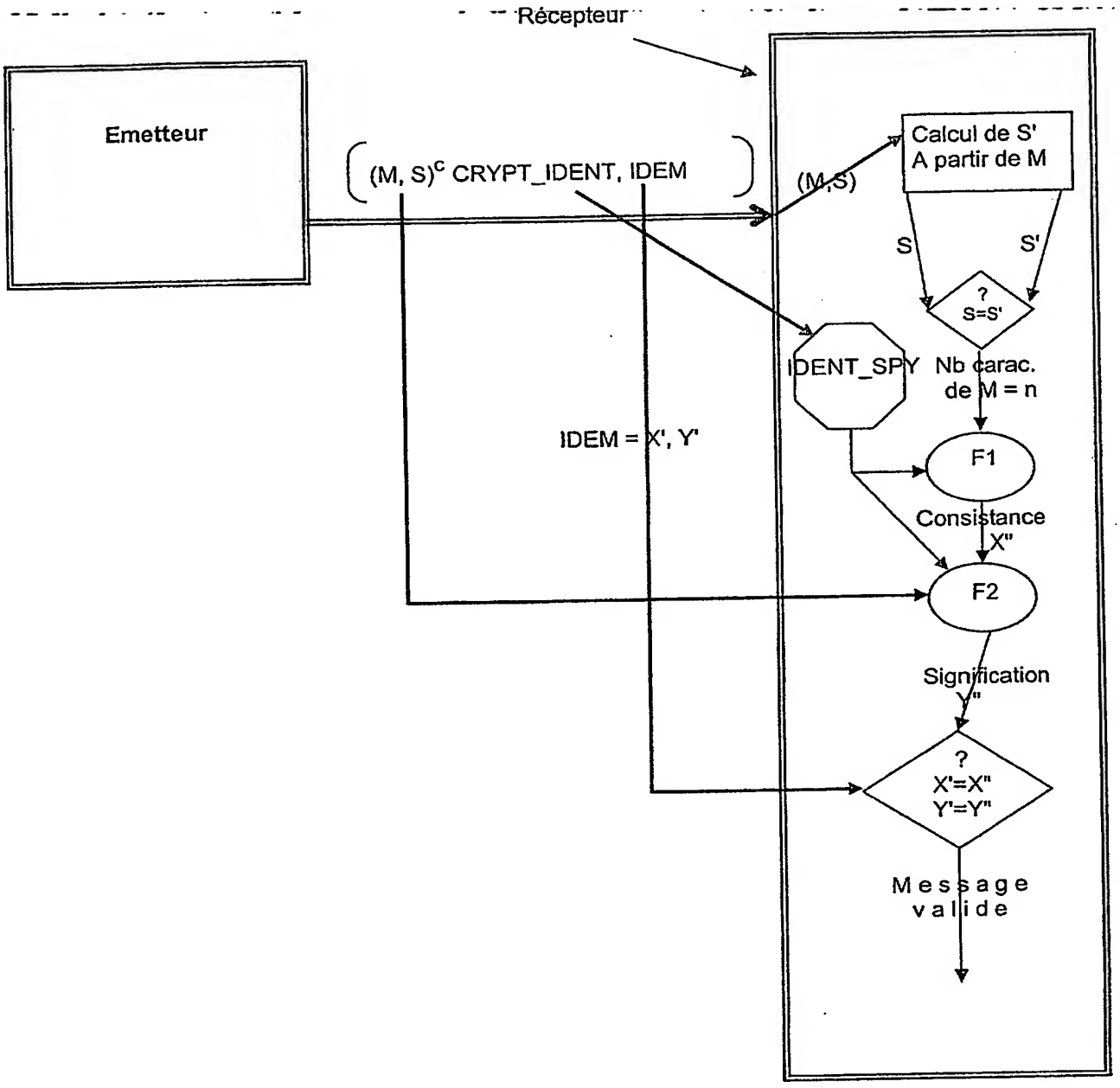

Récepteur
Emetteur
(M, S)^C CRYPT_IDENT, IDEM
(M,S)
Calcul de S'
A partir de M
S
S'
?
S=S'
IDENT_SPY
Nb carac.
de M = n
IDEM = X', Y'
F1
Consistance
X"
F2
Signification
Y"
?
X'=X"
Y'=Y"
Message
valide

Figure 1

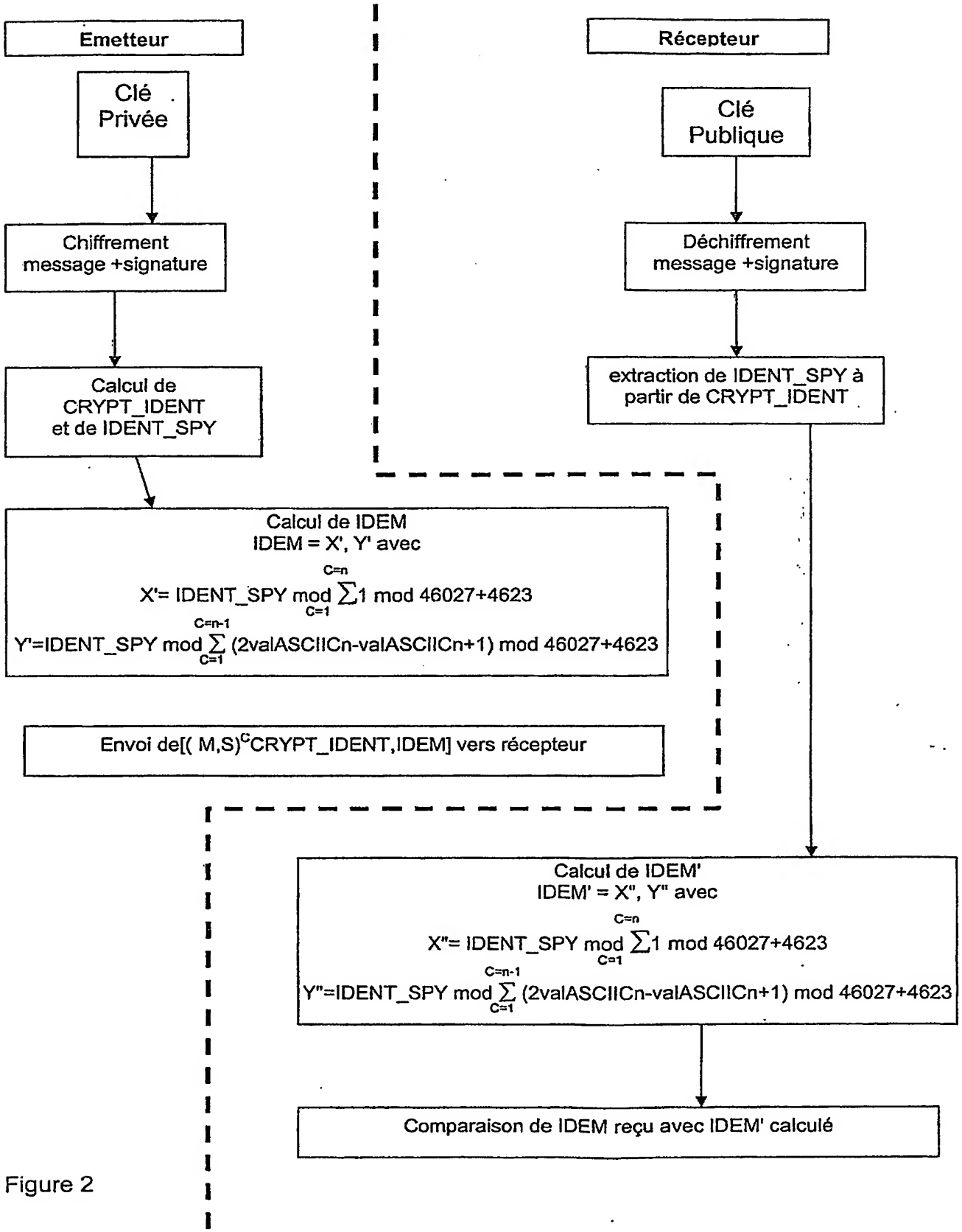

Emetteur
Clé Privée
Chiffrement message +signature
Calcul de CRYPT_IDENT et de IDENT_SPY
Récepteur
Clé Publique
Déchiffrement message +signature
extraction de IDENT_SPY à partir de CRYPT_IDENT
Calcul de IDEM
IDEM = X', Y' avec
X'= IDENT_SPY mod ∑(C=1 à C=n) 1 mod 46027+4623
Y'=IDENT_SPY mod ∑(C=1 à C=n-1) (2valASCIICn-valASCIICn+1) mod 46027+4623
Envoi de[(M,S)^C CRYPT_IDENT,IDEM] vers récepteur
Calcul de IDEM'
IDEM' = X", Y" avec
X"= IDENT_SPY mod ∑(C=1 à C=n) 1 mod 46027+4623
Y"=IDENT_SPY mod ∑(C=1 à C=n-1) (2valASCIICn-valASCIICn+1) mod 46027+4623
Comparaison de IDEM reçu avec IDEM' calculé

Figure 2

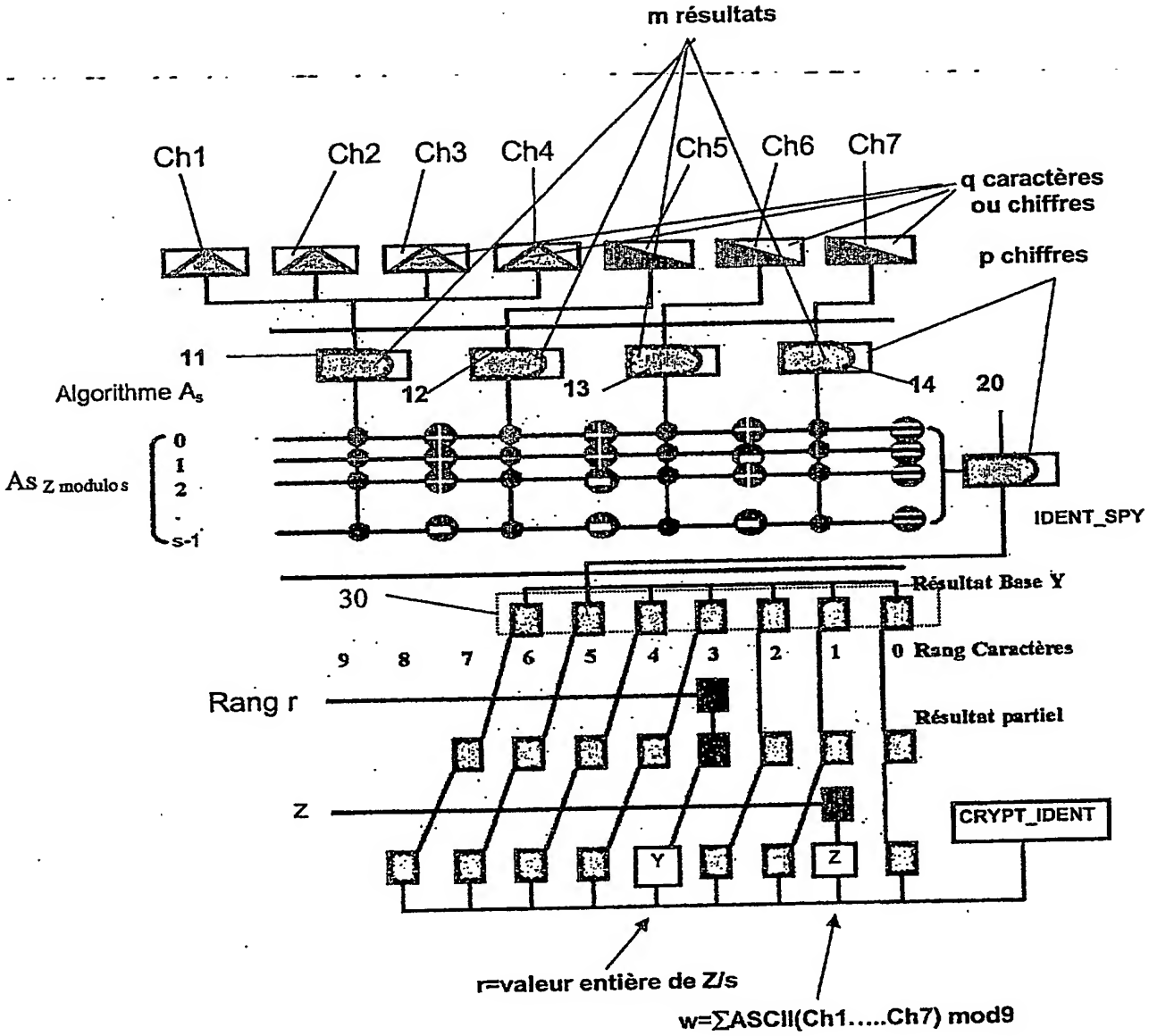
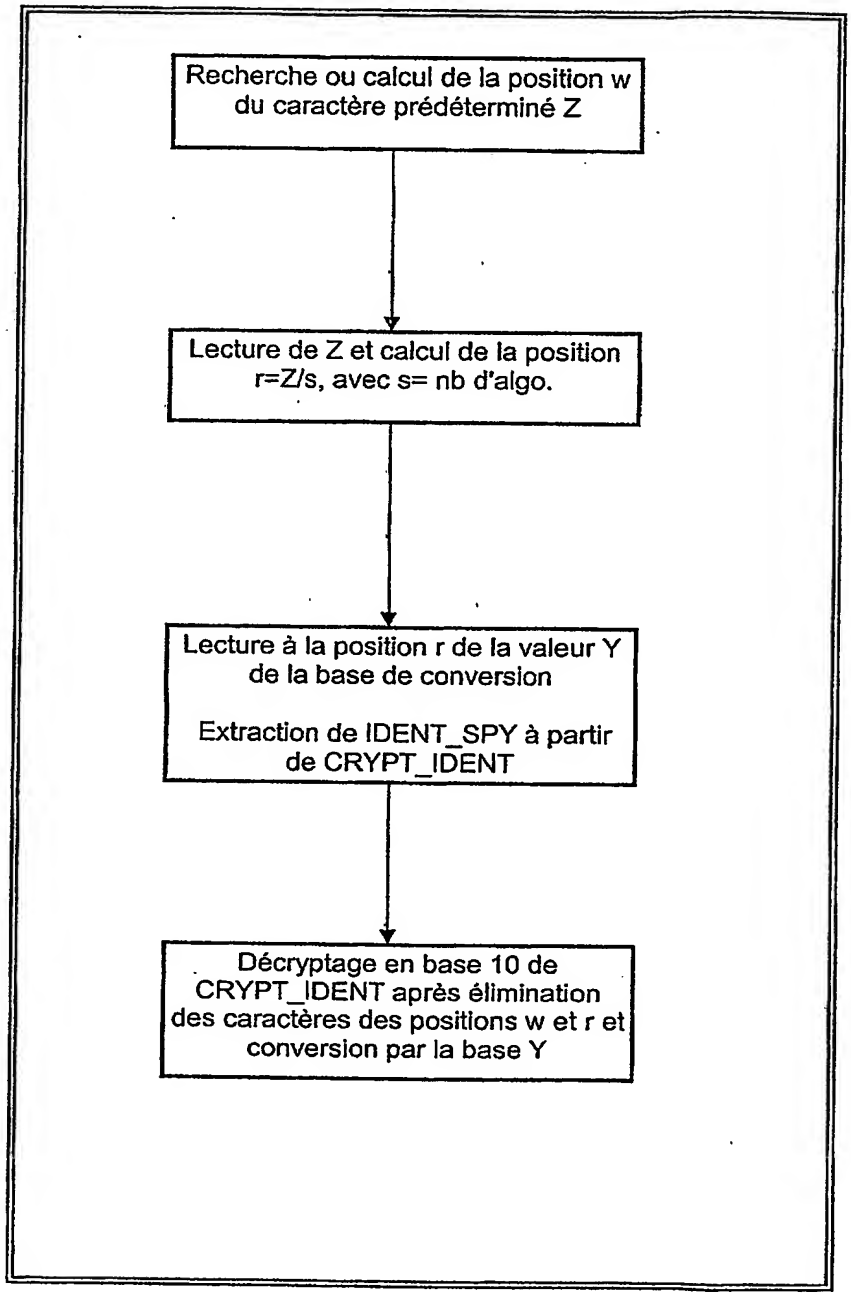

m résultats
Ch1
Ch2
Ch3
Ch4
Ch5
Ch6
Ch7
q caractères ou chiffres
p chiffres
11
12
13
14
20
Algorithme A_s
$A_{S\ Z\ modulo\ s}$
0
1
2
.
s-1
IDENT_SPY
Résultat Base Y
30
9 8 7 6 5 4 3 2 1 0 Rang Caractères
Rang r
Résultat partiel
Z
CRYPT_IDENT
Y
Z
r=valeur entière de Z/s
w=∑ASCII(Ch1.....Ch7) mod9

Figure 3

Figure 4


Recherche ou calcul de la position w du caractère prédéterminé Z
Lecture de Z et calcul de la position r=Z/s, avec s= nb d'algo.
Lecture à la position r de la valeur Y de la base de conversion
Extraction de IDENT_SPY à partir de CRYPT_IDENT
Décryptage en base 10 de CRYPT_IDENT après élimination des caractères des positions w et r et conversion par la base Y